PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-067186
(43)Date of publication of application : 03.03.2000

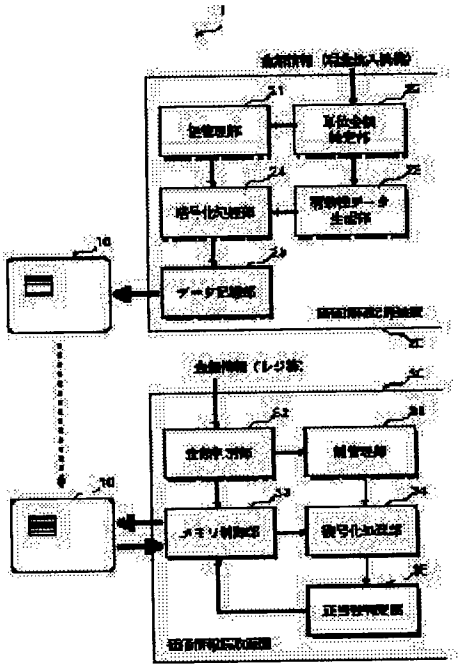
(51)Int.Cl. G06K 17/00
G06F 19/00
G06K 19/00
G07F 7/08

(21)Application number : 10-233771
(22)Date of filing : 20.08.1998

(71)Applicant : NTT DATA CORP
(72)Inventor : HAYASHI SEIICHIRO

(54) ELECTRONIC PAYMENT METHOD, ELECTRONIC PAYMENT SYSTEM AND RECORD MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an electronic payment system which is high in security and eliminates the need to increase a storage area for value information and limit retainable value information.
SOLUTION: Pairs of ciphering keys and deciphering keys which are different by unit money amounts such as 10 yen and 100 yen are determined between a value information recording device 20 and a value information reader 30. The value information recording device 20 generates unit ciphered value data by ciphering effectiveness data showing the effectiveness of a unit money amount with the corresponding ciphering key and records the number of necessary units and unit ciphered value data on an IC card 10. The value information reader 30 reads the number of units and unit ciphered value data out of the IC card 10 and deciphers the effectiveness data with the corresponding deciphering key at the time of payment and when the effectiveness of money mount information is confirmed with the deciphering result, the corresponding unit ciphered value data are deleted from the IC card 10.



LEGAL STATUS

[Date of request for examination] 08.08.2000
[Date of sending the examiner's decision of rejection] 04.03.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－67186
(P2000－67186A)
(43)公開日　平成12年３月３日(2000.3.3)

(51)Int.Cl.[7]	識別記号	FI		テーマコード（参考）
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｒ	３Ｅ０４４
			Ｓ	５Ｂ０３５
Ｇ０６Ｆ　19/00		Ｇ０６Ｆ　15/30	Ｌ	５Ｂ０５５
Ｇ０６Ｋ　19/00		Ｇ０６Ｋ　19/00	Ｕ	５Ｂ０５８
Ｇ０７Ｆ　7/08		Ｇ０７Ｆ　7/08	Ｒ	

審査請求　未請求　請求項の数８　ＯＬ　（全７頁）

(21)出願番号　特願平10－233771

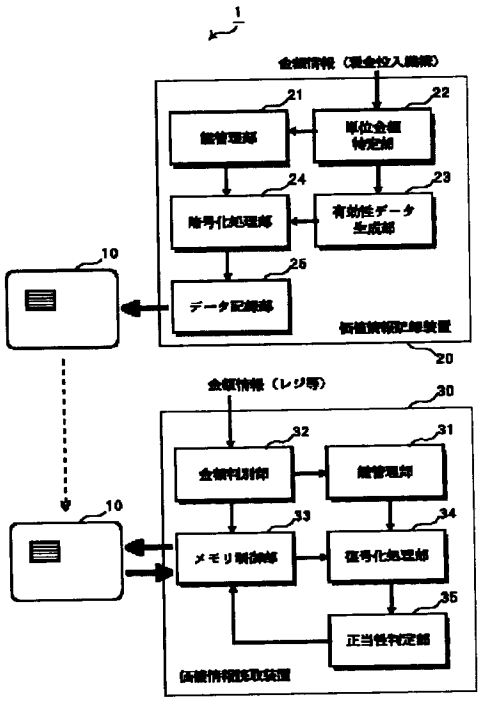
(22)出願日　平成10年８月20日(1998.8.20)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　林　誠一郎
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100099324
弁理士　鈴木　正剛

Ｆターム(参考)　3E044 AA20 BA04 BA06 CA05 CA06
CA10 DA01 DA03 DB02 DC05
5B035 AA13 BB02 BB03 BB09 BC02
CA22 CA23
5B055 BB10 HA14 KK05
5B058 CA13 CA15 KA11 KA31 YA06

(54)【発明の名称】　電子支払方法およびシステム、記録媒体

(57)【要約】
【課題】　価値情報の記憶領域を増大させたり、保有可能な価値情報に制限を設ける必要がない、高セキュリティ性の電子支払システムを提供する。
【解決手段】　価値情報記録装置２０と価値情報読取装置３０との間で、例えば１０円、１００円のような単位金額毎に異なる暗号鍵と復号鍵の対を定めておく。価値情報記録装置２０は、単位金額の有効性を表す有効性データを対応する暗号鍵で暗号化して単位暗号価値データを生成し、所要単位及び数の単位暗号価値データをＩＣカード１０に記録する。価値情報読取装置３０は、支払時に、ＩＣカード１０から該当単位及び数の単位暗号価値データを読み取ってそれぞれ対応する復号鍵で有効性データに復号し、復号結果によって金額情報としての有効性が確認されたときに当該単位暗号価値データをＩＣカード１０より削除する。



【特許請求の範囲】

【請求項１】　支払対象となる電子価値情報の単位価値毎に異なる暗号鍵及び復号鍵の組を定め、個々の単位価値の有効性を表す有効性データを対応する暗号鍵で暗号化して単位暗号価値データを生成し、所要単位及び数の単位暗号価値データを可搬性記録媒体に記録しておく過程と、

支払時に前記可搬性記録媒体から該当単位及び数の単位暗号価値データを読み取ってそれぞれ対応する復号鍵で前記有効性データに復号し、該復号結果により電子価値情報の有効性が確認されたときに当該単位暗号価値データを前記可搬性記録媒体より削除する過程と、を含む電子支払方法。

【請求項２】　可搬性記録媒体と、この可搬性記録媒体への電子価値情報の記録を行う価値情報記録装置と、前記可搬性記録媒体に記録された電子価値情報の読み取りおよび削除を行う価値情報読取装置とを備え、前記価値情報記録装置と前記価値情報読取装置との間で、電子価値情報の単位価値毎に異なる暗号鍵と復号鍵の対が定められたシステムであって、

前記価値情報記録装置は、個々の単位価値の有効性を表す有効性データを対応する暗号鍵で暗号化して単位暗号価値データを生成し、所要単位及び数の単位暗号価値データを前記可搬性記録媒体に記録するように構成され、

前記価値情報読取装置は、電子支払発生時に、前記可搬性記録媒体から該当単位及び数の単位暗号価値データを読み取ってそれぞれ対応する復号鍵で前記有効性データに復号し、該復号結果によって電子価値情報の有効性が確認されたときに当該単位暗号価値データを前記可搬性記録媒体より削除するように構成されていることを特徴とする電子支払システム。

【請求項３】　前記価値情報記録装置は、予め支払目的に応じた単位暗号価値データを生成しておき、任意の種別及び数の単位暗号価値データを前記可搬性記録媒体に記録するように構成されていることを特徴とする請求項２記載の電子支払システム。

【請求項４】　前記可搬性記録媒体が、書換可能な記録領域を有するカード状記録媒体であることを特徴とする請求項２または３記載の電子支払システム。

【請求項５】　電子価値情報の単位価値毎に異なる暗号鍵および復号鍵の組を定めるとともに前記暗号鍵を保有する鍵管理手段と、

記録対象となる単位価値の種別および数を特定する手段と、

特定した種別および数の単位価値の有効性を表す有効性データを対応する暗号鍵で暗号化して単位暗号価値データを生成する手段と、

この単位暗号価値データを可搬性記録媒体に記録する手段とを備え、

前記可搬性記録媒体に記録された単位暗号価値データを前記復号鍵でのみ復号できるようにした価値情報記録装置。

【請求項６】　請求項５記載の価値情報記録装置によって前記単位暗号価値データが記録された可搬性記録媒体から該当単位及び数の単位暗号価値データを読み取る手段と、

読み取った単位暗号価値データを当該単位暗号価値データの暗号化に用いられた暗号鍵に対応する復号鍵で復号し、該復号結果によって電子価値情報の有効性を確認したときに当該単位暗号価値データを前記可搬性記録媒体より削除する手段とを有する価値情報読取装置。

【請求項７】　電子価値情報の単位価値毎に異なる暗号鍵と復号鍵の組を定めるとともに、前記復号鍵を知得した価値情報読取装置により読み取られる可搬性記録媒体を装着する手段を有するコンピュータ装置に下記の処理を実行させるためのプログラムコードが記録されたコンピュータ読取可能な記録媒体。

（１）記録対象となる単位価値の種別および数を特定する処理、（２）特定した種別および数の単位価値の有効性を表す有効性データを、対応する暗号鍵で暗号化して単位暗号価値データを生成する処理、（３）前記生成された単位暗号価値データを前記可搬性記録媒体へ記録する処理。

【請求項８】　請求項５記載の価値情報記録装置によって前記単位暗号価値データが記録された可搬性記録媒体を装着する手段を有するコンピュータ装置に下記の処理を実行させるためのプログラムコードが記録されたコンピュータ読取可能な記録媒体。

（１）前記可搬性記録媒体から該当単位及び数の単位暗号価値データを読み取る処理、（２）読み取った単位暗号価値データを当該単位暗号価値データの暗号化に用いられた暗号鍵に対応する復号鍵で復号する処理、（３）該復号結果によって電子価値情報の有効性を確認したときに当該単位暗号価値データを前記可搬性記録媒体より削除する処理。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子マネー、電子決済、電子チケット、電子印紙等としての利用に適した電子支払システムに係り、より詳しくは、金額情報や回数券情報、チケット情報等、単位価値毎に特定可能な価値情報を可搬性記録媒体に記録して当該価値情報単位の支払を電子的に行うシステムおよびその関連技術に関する。

【０００２】

【発明の背景】価値を表現する情報、例えば金額情報や回数券情報、チケット情報等（以下、これらを「価値情報」と称する）を秘密鍵を用いて暗号化してＩＣカード等に記録させておき、支払い時や回数券等の使用時に、記録された暗号情報を復号化して電子的な支払いを行う

電子支払システムが知られている。このような電子支払システムでは、復号化後に支払額や使用回数分を価値情報から減算した後、再び秘密鍵で暗号化して再記録しているのが通常である。そのため、秘密鍵をＩＣカード内、もしくはＩＣカードの読取装置側で保有しなければならず、セキュリティ性に欠けるという問題があった。

【０００３】価値情報を暗号化してＩＣカードに複数保有しておくことで上記問題点を解決することが考えられるが、そうすると価値情報そのものを暗号化して保有することになり、そのための記録領域の容量が増大し、もしくは、記録容量の制約から保有可能な価値情報、例えば使用可能な金額の値が制限されてしまう。

【０００４】そこで本発明の課題は、価値情報のセキュリティ性を確保しつつそれを保有しておくための記憶領域を増大させず、保有可能な価値情報の制限もない、改良された電子支払方法を提供することにある。本発明の他の課題は、上記電子支払方法を応用した電子支払システムおよびこの電子支払システムをコンピュータ装置で実現するための記録媒体を提供することにある。

【０００５】

【課題を解決するための手段】上記課題を解決する本発明の電子支払方法は、支払対象となる電子価値情報の単位価値毎に異なる暗号鍵及び復号鍵の組を定め、個々の単位価値の有効性を表す有効性データを対応する暗号鍵で暗号化して単位暗号価値データを生成し、所要単位及び数の単位暗号価値データを可搬性記録媒体に記録しておく過程と、支払時に前記可搬性記録媒体から該当単位及び数の単位暗号価値データを読み取ってそれぞれ対応する復号鍵で前記有効性データに復号し、該復号結果により電子価値情報の有効性が確認されたときに当該単位暗号価値データを前記可搬性記録媒体より削除する過程と、を含む。ここで「支払」とは自己が保有する価値情報を相手側に渡すこと全般を指している。

【０００６】また、上記他の課題を解決する本発明の電子支払システムは、可搬性記録媒体と、この可搬性記録媒体への電子価値情報の記録を行う価値情報記録装置と、前記可搬性記録媒体に記録された電子価値情報の読み取りおよび削除を行う価値情報読取装置とを備え、前記価値情報記録装置と前記価値情報読取装置との間で、電子価値情報の単位価値毎に異なる暗号鍵と復号鍵の対が定められたシステムである。この電子システムにおいて、前記価値情報記録装置は、個々の単位価値の有効性を表す有効性データを対応する暗号鍵で暗号化して単位暗号価値データを生成し、所要単位及び数の単位暗号価値データを前記可搬性記録媒体に記録するように構成されたものであり、前記価値情報読取装置は、電子支払発生時に、前記可搬性記録媒体から該当単位及び数の単位暗号価値データを読み取ってそれぞれ対応する復号鍵で前記有効性データに復号し、該復号結果によって電子価値情報の有効性が確認されたときに当該単位暗号価値データを前記可搬性記録媒体より削除するように構成されたものである。

【０００７】前記価値情報記録装置は、予め支払目的に応じた単位暗号価値データを生成しておき、任意の種別及び数の単位暗号価値データを前記可搬性記録媒体に記録するように構成することもできる。

【０００８】好ましくは、前記可搬性記録媒体を、書換可能な記録領域を有するカード状記録媒体で構成する。

【０００９】前記価値情報記録装置は、具体的には、電子価値情報の単位価値毎に異なる暗号鍵および復号鍵の組を定めるとともに前記暗号鍵を保有する鍵管理手段と、記録対象となる単位価値の種別および数を特定する手段と、特定した種別および数の単位価値の有効性を表す有効性データを対応する暗号鍵で暗号化して単位暗号価値データを生成する手段と、この単位暗号価値データを可搬性記録媒体に記録する手段とを備え、前記可搬性記録媒体に記録された単位暗号価値データを前記復号鍵でのみ復号できるようにしたものである。

【００１０】また、前記価値情報読取装置は、具体的には、前記価値情報記録装置によって単位暗号価値データが記録された可搬性記録媒体から該当単位及び数の単位暗号価値データを読み取る手段と、読み取った単位暗号価値データを当該単位暗号価値データの暗号化に用いられた暗号鍵に対応する復号鍵で復号し、該復号結果によって電子価値情報の有効性を確認したときに当該単位暗号価値データを前記可搬性記録媒体より削除する手段とを有するものである。

【００１１】このような価値情報記録装置および価値情報読取手段をコンピュータ装置で実現するため、本発明は、下記の２種類の記録媒体を提供する。第１の記録媒体は、電子価値情報の単位価値毎に異なる暗号鍵と復号鍵の組を定めるとともに、前記復号鍵を知得した価値情報読取装置により読み取られる可搬性記録媒体を装着する手段を有するコンピュータ装置に下記の処理を実行させるためのプログラムコードが記録されたコンピュータ読取可能な記録媒体である。

（１－１）記録対象となる単位価値の種別および数を特定する処理、（１－２）特定した種別および数の単位価値の有効性を表す有効性データを、対応する暗号鍵で暗号化して単位暗号価値データを生成する処理、（１－３）前記生成された単位暗号価値データを前記可搬性記録媒体へ記録する処理。

【００１２】第２の記録媒体は、前記価値情報記録装置によって前記単位暗号価値データが記録された可搬性記録媒体を装着する手段を有するコンピュータ装置に下記の処理を実行させるためのプログラムコードが記録されたコンピュータ読取可能な記録媒体である。

（２－１）前記可搬性記録媒体から該当単位及び数の単位暗号価値データを読み取る処理、（２－２）読み取った単位暗号価値データを当該単位暗号価値データの暗号

化に用いられた暗号鍵に対応する復号鍵で復号する処理、（２－３）該復号結果によって電子価値情報の有効性を確認したときに当該単位暗号価値データを前記可搬性記録媒体より削除する処理。

【００１３】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。図１は、本発明を適用した電子支払システムの構成図である。この電子支払システム１は、可搬性記録媒体の一例となるＩＣカード１０と、このＩＣカード１０の記録領域に電子価値情報を書き込む価値情報記録装置２０と、ＩＣカード１０との間で価値情報の読取に関わるデータ類の送受を行う価値情報読取装置３０とを含んで構成される。

【００１４】ここでは、電子価値情報を金額情報とし、ＩＣカード１０をプリペイドカードとして利用する場合の例を示す。価値情報記録装置２０には、利用者による現金投入機構または利用者の金融機関の口座との連絡機構が設けられている。価値情報読取装置３０は、サービス提供機関や店舗等に備えられ、通常、ＰＯＳシステム等が接続されている。また、単位金額毎に、暗号鍵及び復号鍵の対を定めておき、価値情報記録装置２０には暗号鍵を、価値情報読取装置３０側では復号鍵を保有しておく。より一般的には、暗号鍵は価値情報記録装置２０の秘密鍵であり、復号鍵は、その秘密鍵に対応した公開鍵であるが、常にこのようにしなければならないというものではなく、秘密鍵方式を採用することもできる。

【００１５】ＩＣカード１０は、書換可能なメモリ領域を有する汎用のものである。価値情報記録装置２０は、ＩＣカード用のリーダライタを具備したコンピュータ装置によって実現されるもので、そのコンピュータ装置が所定のプログラムコードを読み込んで実行することにより形成される、鍵管理部２１、単位金額特定部２２、有効性データ生成部２３、暗号化処理部２４、データ記録部２５の機能ブロックを有している。

【００１６】鍵管理部２１は、前述の暗号鍵を単位金額毎に保有している。単位金額特定部２２は単位金額（１円、５円、１０円、５０円、１００円、５００円、１，０００円等）の種別および数を特定するものであり、有効性データ生成部２３は、対象となる金額情報（単位金額を含む）の有効性を表す有効性データを生成するものである。有効性データは１ビット程度の任意のデータであり、通常は、単位金額毎に異なるデータ（例えば１０円であれば“３”、１００円であれば“５”等）が用いられる。単位金額特定部２２では、通常は、有効性データの数が最小になるように単位金額の種別が特定されるようになっている。但し、利用者が指定した場合はその指定内容による。

【００１７】暗号化処理部２４は、生成された有効性データをその単位金額に対応する暗号鍵で暗号化して単位暗号価値データを生成するものである。データ記録部２５は、生成された単位暗号価値データのＩＣカード１０の記録領域への書き込み、つまり支払可能な金額情報のチャージを行うものである。

【００１８】価値情報読取装置３０もまた、ＩＣカード用のリーダライタを具備したコンピュータ装置によって実現されるもので、そのコンピュータ装置が所定のプログラムコードを読み込んで実行することにより形成される、鍵管理部３１、金額判別部３２、メモリ制御部３３、復号化処理部３４、正当性判定部３５の機能ブロックを少なくとも有している。

【００１９】鍵管理部３１は、上記暗号鍵に対応した単位金額毎の復号鍵を保有している。金額判別部３２は、入力された金額情報、つまり支払要求合計額から必要な単位金額の種別および数を判別するものである。メモリ制御部３３は、判別されたそれぞれの単位金額に対応する単位暗号価値データをリーダライタを通じてＩＣカード１０のメモリ領域より読み出すとともに、後述するように金額情報の有効性が認められた場合は、該当する単位暗号価値データをメモリ領域を削除するものである。

【００２０】復号化処理部３４は、取得した単位暗号価値データを復号鍵を用いて有効性データに復号するものである。正当性判定部３５は、復号された有効性データをもとに金額情報の正当性、すなわち金額情報として扱うことの妥当性を確認するものである。

【００２１】なお、上記各機能ブロックを実現するためのプログラムコードは、通常、各コンピュータ装置のＣＰＵが読取可能な固定記録媒体に随時読み取り可能な形態で記録されたものであるが、可搬性の記録媒体、例えばフレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ、磁気テープに記録され、あるいはコンピュータがアクセス可能なプログラムサーバや半導体メモリに記録されて、運用時に上記固定記録媒体にインストールされるものであっても良い。また、上記プログラムコードのみを実行することによって上記各機能ブロックが形成されるだけでなく、そのプログラムコードの指示に基づいて当該コンピュータ装置上で稼働しているオペレーティングシステムが実際の処理の一部を行い、その処理を通じて上記各機能ブロックが形成されるものであっても良い。本発明の記録媒体は、上記のようなプログラムコードをコンピュータ読取可能な形態で記録したものである。

【００２２】次に、上記電子支払システム１における実際の運用形態を、図２～図４を参照して具体的に説明する。便宜上、単位金額を１０円、１００円とし、１０円について秘密鍵Ｋｓ１０と公開鍵Ｋｐ１０，１００円について秘密鍵Ｋｓ１００と公開鍵Ｋｐ１００の組を割り当て、秘密鍵ｋｓ１０，ｋｓ１００については価値情報記録装置２０の鍵管理部２１に保有しておく。公開鍵Ｋｐ１０，Ｋｐ１００については、価値情報記録装置２０

に配布してその鍵管理部２１に保有しておく。ここでは、利用者がＩＣカード１０に４５０円分の金額情報をチャージし、店舗で１４０円分の消費を行った場合を例に挙げて説明する。

【００２３】価値情報記録装置２０におけるＩＣカード１０への金額情報のチャージは、図２の手順で行われる。

【００２４】すなわち、価値情報記録装置２０では、利用者がＩＣカード１０をカードリーダに装着して現金投入機構に現金４５０円を投入したことを確認すると（ステップＳ１０１：Yes、Ｓ１０２：Yes）、単位金額特定部２２で４５０円分の単位金額の種別および数を特定する。ここでは、１００円が4つ、１０円が5つのように特定される（ステップＳ１０３）。

【００２５】有効性データ生成部２３は、それぞれの単位金額についての有効性データＶを生成し、これを暗号化処理部２４に送る（ステップＳ１０４）。暗号化処理部２３は、鍵管理部２１から１０円の秘密鍵ｋｓ１０と１００円の秘密鍵ｋｓ１００を読み出し、各有効性データＶを暗号化して単位暗号価値データを生成する。１０円についての単位暗号化価値データを「Ｅｋｓ１０［Ｖ］」、１００円についての単位暗号化価値データを「Ｅｋｓ１００［Ｖ］」とする（ステップＳ１０５）。データ記録部２５は、5つの単位暗号価値データＥｋｓ１０［Ｖ］と、4つの単位暗号価値データＥｋｓ１００［Ｖ］をＩＣカード１０のメモリ領域へ記録する（ステップＳ１０６）。その後、図示しない表示装置を通じて利用者に正常チャージ通知を行い（ステップＳ１０７）、処理を終える。

【００２６】このようにして金額情報がチャージされたＩＣカード１０のメモリ領域の状態を図４（ａ）に示す。参照符号１１はメモリ領域である。メモリ領域１１は、図示のように、単位金額毎に単位暗号化価値データが順次蓄積されるようになっている。

【００２７】図３は、店舗に設置された価値情報読取装置２０の処理手順図である。電子支払は、この図３の手順で行われる。

【００２８】すなわち価値情報読取装置３０のリーダライタにＩＣカード１０が装着され、且つレジ等で金額情報が入力されたことを確認すると（ステップＳ２０１：Yes、Ｓ２０２：Yes）、価値情報読取装置３０は、金額判別部３２でその金額情報が１００円が１つと１０円が４つの組み合わせから成ることを判別する（ステップＳ２０３）。そして、メモリ制御部３３を通じて残高チェック、つまり単位暗号化価値データによる支払が可能かどうかをチェックする（ステップＳ２０４）。支払が可能な場合は、該当種別および数の単位価値暗号データを取得し、これらを復号化処理部３４に送る（ステップＳ２０５：Yes、Ｓ２０６）。本例では、１つの単位暗号化価値データＥｋｓ１００［Ｖ］と４つの単位暗号価値データＥｋｓ１０［Ｖ］をＩＣカード１０のメモリ領域から取得する。

【００２９】復号化処理部３４は、鍵管理部３１から１００円の公開鍵Ｋｐ１００と１０円の公開鍵Ｋｐ１０を読み出し、これらを用いて各単位暗号化価値データＥｋｓ１００［Ｖ］、Ｅｋｓ１０［Ｖ］から有効性データＶを復号する（ステップＳ２０７）。そして、正当性判定部３５で、復号結果である金銭情報の有効性を確認する（ステップＳ２０８）。

【００３０】有効性が確認された場合は、図示しない表示装置を通じて利用者に支払完了を通知するとともに、メモリ制御部３３を通じて、読み込んだだけの単位暗号価値データＥｋｓ１００［Ｖ］、Ｅｋｓ１０［Ｖ］をＩＣカード１０のメモリ領域１１から削除する（ステップＳ２０８：Yes、Ｓ２０９）。このときのＩＣカード１０のメモリ領域の状態は図４（ｂ）に示すようになる。破線で示した部分が削除された単位暗号価値データである。削除された部分は、新たな金額情報をチャージする領域として使用可能となる。

【００３１】なお、ステップＳ２０５において支払が不能であった場合、あるいはステップＳ２０８で有効性が認められなかった場合は、支払不能であった旨を利用者に通知し、さらに、リーダライタを制御してＩＣカード１０を排出させる（ステップＳ２０５：No、Ｓ２０８：No、Ｓ２１０）。

【００３２】このように、本実施形態の電子支払システム１では、単位金額毎に異なる暗号鍵及び復号鍵の組を定め、個々の単位金額の有効性を表す１ビット程度の有効性データを対応する暗号鍵で暗号化して単位暗号価値データを生成し、所要単位及び数の単位暗号価値データをＩＣカード１０に記録しておき、電子支払発生時には、このＩＣカード１０から該当単位及び数の単位暗号価値データを読み取ってそれぞれ対応する復号鍵で有効性データに復号し、該復号結果により金額情報としての有効性が確認されたときに各単位暗号価値データをＩＣカード１０から削除するようにしたので、ＩＣカード１０自体には、鍵を保有させる必要がなくなり、取引の安全性が十分に確保できるようになる。

【００３３】また、単位暗号化価値データは、有効性を表現する最低１ビットだけで良いので、ＩＣカードのメモリ容量を増大させることもなく、チャージ可能な支払単位金額の制約もない。これにより、従来の問題点が解消される。

【００３４】なお、本実施形態では、価値情報記録装置２０において、金額情報の入力を契機に単位金額を特定し、特定した分の有効性データを暗号化して単位暗号価値データＶを生成する場合の例を示したが、支払目的に応じた単位暗号価値データを予め生成しておき、任意の種別及び数の単位暗号価値データを選択してＩＣカード１０に記録するようにしても良い。

9

【００３５】また、本実施形態では、電子価値情報として金額情報を例に挙げて説明したが、回数券、チケット、印紙類のように、単位価値を特定できる用途全般に対しても、本実施形態と同様に適用が可能である。

【００３６】また、本実施形態では、可搬性記録媒体として書換可能なＩＣカード１０を用いたが、ハイブリッドカード、光カード、半導体メモリカードその他のカード状記録媒体を用いても良く、特に書換を要しない場合には、磁気カードのように安価なカード状記録媒体であっても良い。

【００３７】さらに、接触型カード媒体のほか、非接触型カード媒体を用いて本発明を実施することが可能である。但し、この場合は、価値情報記録装置２０や価値情報読取装置３０側に非接触型カード媒体との間で情報の授受を行うことができるリーダライタを設ける必要がある。

【００３８】

【発明の効果】以上の説明から明らかなように、本発明によれば、価値情報のセキュリティ性を確保しつつ価値情報を保有しておくための記憶領域を増大させず、保有可能な価値情報の制限もなくなるという特有の効果がある。

【図面の簡単な説明】

10

＊【図１】本発明を適用した電子支払システムの機能構成図。

【図２】本実施形態による金額チャージ処理の手順図。

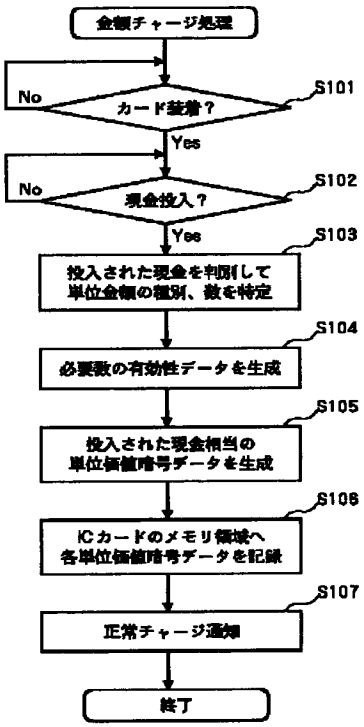
【図３】本実施形態による支払時の処理手順図。

【図４】（ａ）は金額チャージを終えたときのメモリ領域の状態、（ｂ）は支払を終えたときのメモリ領域の状態を示した説明図。

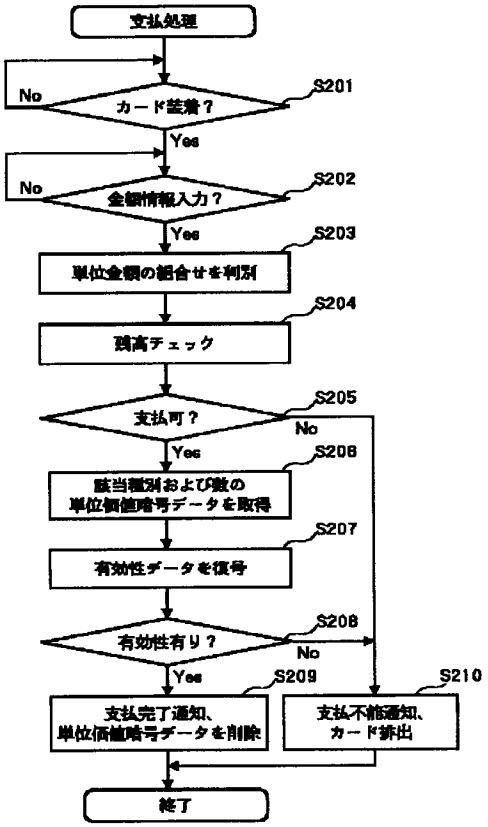
【符号の説明】

１　電子支払システム
１０　ＩＣカード
１１　ＩＣカードのメモリ領域
２０　価値情報記録装置
２１　鍵管理部
２２　単位金額特定部
２３　有効性データ生成部
２４　暗号化処理部
２５　データ記録部
３０　価値情報読取装置
３１　鍵管理部
３２　金額判別部
３３　メモリ制御部
３４　復号化処理部
３５　正当性判定部

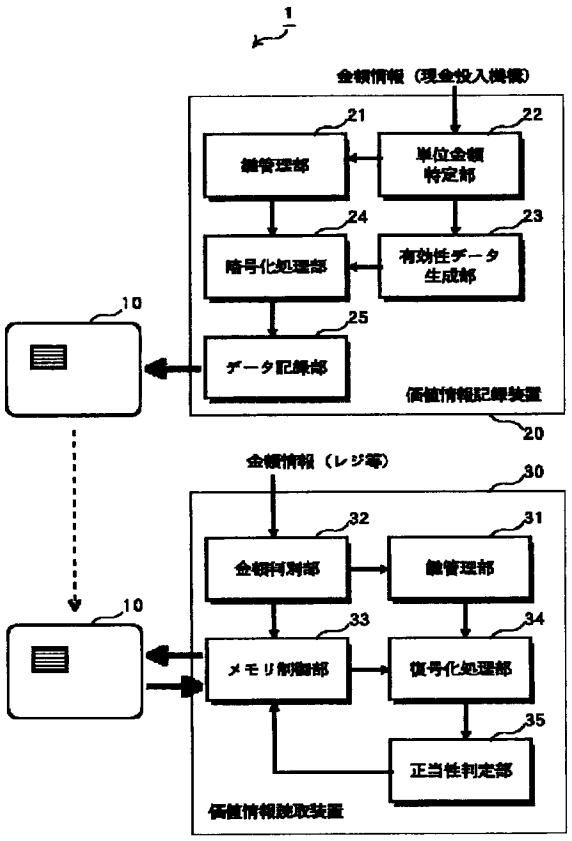
【図２】



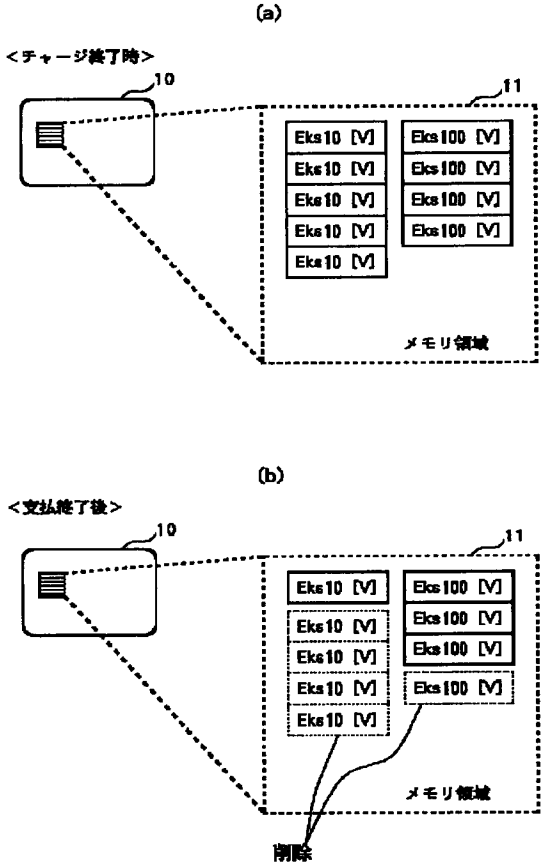
【図３】



【図１】


1
金額情報（現金投入機械）
21
22
値管理部
単位金額特定部
24
23
暗号化処理部
有効性データ生成部
25
データ記録部
価値情報記録装置
20
10
金額情報（レジ等）
30
32
31
金額判別部
値管理部
33
34
メモリ制御部
復号化処理部
35
正当性判定部
価値情報読取装置
10

【図４】


(a)
<チャージ終了時>
10
11
Eks10 [V]
Eks100 [V]
メモリ領域
(b)
<支払終了後>
削除